REMARKS

Applicant respectfully thanks Examiner Leynna for having an interview held on November 5, 2008 to discuss an applicant's proposed amendment as now proposed herewith.

Applicant responds hereby to the office action dated September 16, 2008. Claims 3, 8 and 15 are amended hereby. Claims 1-2, 6-7, 12, and 20-22 were previously cancelled without prejudice or disclaimer of subject matter. Claim 24-25 are newly added without entering new matter. Claims 3-5, 8-11, 13-19, and 23-25 remain pending hereinafter, where Claims 3, 8 and 15 are independent claims.

Favorable consideration and allowance of the claims of the present application are respectfully requested.

Rejections under 35 U.S.C. § 103(a)

The Examiner rejects Claims 3-5, 8-11, 13-19 and 23 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Ellison, et al. (US 7,380,278 B2) (hereinafter "Ellison") further in view of Teal, et al. (US 7,398,389 B2) (hereinafter "Teal").

In response, Claims 3, 8 and 15 are being amended to recite "at a kernel layer" at every method step. During the interview, Examiner suggested clarifying that every method step is performed in the kernel layer. In the way, the claimed invention can be patentably distinct over Ellison, Teal, whether alone or in a combination. The added limitation ("at the kernel layer" at every method step) is supported at Figure 6 and a paragraph [0052] of the corresponding Pre-Granted Publication (US 2005/0022026 A1). Specifically, the paragraph [0052] states, "In general, embodiments of the present invention may be installed in one or more of data processing layers 600-630. Each installation then protects the layer in which it is hosted from corruption". Thus, the paragraph [0052] supports that all the method steps are implemented in the kernel layer 620. Therefore, no new matter is entered.

For example, amended Claims 3 and 8 states, "providing, at the kernel layer, an initial secrete". On the other hand, col. 9, lines 4-7 and FIG. 2 of Ellison describes, "the BK0 202 is generated at random when the processor nub 18 is first invoked, i.e., when it is first executed on the secure platform". The processor nub 18 of Ellison is not in a kernel layer. FIG. 1B and Col.

3, lines 13-23 of Ellison clearly describes that the processor nub 18 is not in Ring-0 11 (kernel) but in an isolated execution Ring-0 15. Thus, "providing, at the kernel layer, an initial secrete" is not taught by Ellison. Though Teal illustrates a kernel space in Figure 1, Teal fails to discuss "providing, at the kernel layer, an initial secret". A combination of Ellison and Teal neither discuss "providing, at the kernel layer, an initial secret". As another example, amended Claims 3 and 8 states, "at the kernel layer, generating a new secret by performing the collision resistant cryptographic function on a combination of data indicative of the administrative action and the previous secret". Amended Claim 15 states, "updating, at the kernel layer, the initial secret in advance of an administrative action by computing a new secret". On the other hand, col. 9, lines 14-16 and FIG. 2 of Ellison describes, "the key generator 240 generates the OSNK 203 by combining the BK0 202 and the OS Nub ID 201 using a cryptographic hash function". However, the key generator 240 of Ellison is not in a Ring-0 11, which is a kernel. FIG. 2 of Ellison clearly illustrates the key generator 240 is a separate entity, which does not belong to an OS nub 16 or software environment 210. Though Teal illustrates a kernel space in Figure 1, Teal fails to discuss "at the kernel layer, generating a new secret by performing the collision resistant cryptographic function on a combination of data indicative of the administrative action and the previous secret" required amended Claims 3 and 8 or "updating, at the kernel layer, the initial secret in advance of an administrative action by computing a new secret" required amended Claim 15. A combination of Ellison and Teal neither discuss "at the kernel layer, generating a new secret by performing the collision resistant cryptographic function on a combination of data indicative of the administrative action and the previous secret" required amended Claims 3 and 8 or "updating, at the kernel layer, the initial secret in advance of an administrative action by computing a new secret" required amended Claim 15. Though Applicant provide two examples, other method steps executed in the kernel layer are not taught or suggested by Ellison, Teal, whether alone or in a combination.

Claims 3, 8 and 15 are further being amended to recite "**collision resistant** cryptographic function". The paragraph [0040] of the corresponding Pre-Granted Publication (US 2005/0022026 A1) provides a definition of "collision resistant". Though Ellison discusses a cryptographic hash function at col. 9 lines 16 and 22, Ellison fails to discuss "**collision resistant** cryptographic function". Teal discusses a cryptographic digital hash at claims 8 and 36.

However, Teal neither discusses "**<u>collision resistant</u>** cryptographic function". Hence, Ellision, Teal, whether alone or in a combination fails to discuss "collision resistant cryptographic function" required in amended Claims 3 and 8.

Claims 3, 8 and 15 are further being amended to recite "**<u>recording the new secret in a place of the previous secret</u>**". The added subject matter is found at paragraphs [0027] and [0035] of the corresponding Pre-Granted Publication. Therefore, no new matter is entered. Ellison states at col. 9 lines 14-16, "the key generator 240 generates the OSNK 203 by combining the BK0 202 and the OS Nub ID 201 using a cryptographic hash function". Figure 2 of Ellison also illustrates that the key generator 240 generates the OSNK 203 based on the OS Nub ID 201 and the BK0 202. However, the OSNK 203 does not overwrite the BK0 202. Figure 2 of Ellison clearly illustrates that the OSNK 203 is provided to the usage protector 250, not to the processor nub 18. Col. 9, lines 8-9 also states, "a key operating system nub key (OSNK) 203 which is provided only to the OS Nub 16. The OS nub 16 may supply the OSNK 203 to trusted agents, such as the usage protector 250". Thus, the OSNK 203 is provided to the usage protector 250 and/or to the OS Nub 16. The OSNK 203 is not provided to the processor nub 18, which includes the BK0 202. However, amended Claims 3, 8 and 15 state, "recording the new secret in a place of the previous secret". Hence, the added limitation is not taught or suggested by Ellison. Teal does not discuss any subject matter related to generating a secret or recording a secret. Thus, Ellison, Teal, whether alone or in a combination, fails to discuss "<u>recording the new secret in a place of the previous secret</u>" required in amended Claims 3, 8 and 15.

The Examiner alleges that col. 2, lines 52-65 and col.3 lines 11-20 of Ellison teaches or suggests "the kernel layer between a hardware layer and an operating system layer" required in Claims 3, 8 and 15. Col. 2, lines 52-65 and col. 3, lines 11-20 of Ellison discusses ring-0, ring-1, ring-2 and ring-3. Specifically, col. 3, lines 13-15 of Ellison states, "Ring-0 11 includes software modules that are critical for the operating system, usually referred to as kernel". Col. 3, lines 17-20 of Ellison states, "the isolated execution Ring-0 15 includes an operating system (OS) nub 16 and a processor nub 18. The OS nub 16 and the processor nub 18 are instances of an OS executive (OSE) and processor executive (PE), respectively". Figure 1B of Ellison illustrates that the ring-0 11 (kernel) is separated from the ring-0 15 including the OS nub 16 and the processor nub 18. Furthermore, the processor nub 18 is not a hardware layer. The processor nub 18 is a software entity stored in a memory as illustrated in Figure 1C of Ellison. Thus, Ellison fails to teach or suggest "the kernel layer between a hardware layer and an operating system layer" required in Claims 3, 8 and 15. Teal also fails to teach or suggest "the kernel layer between a hardware layer and an operating system layer". Thus, Ellison, Teal, whether alone or in a combination, fails to teach or suggest "the kernel layer between a hardware layer and an operating system layer" required in Claims 3, 8 and 15.

The Examiner alleges that col. 9, lines 10-43 and col. 11, lines 40-48 of Ellison teaches or suggests "erasing the previous secret" required in Claims 3 and 8 and "erasing the initial secret together with any information from which the initial secret might be derived" required in Claim 15. Col. 11, lines 40-48 of Ellison discusses "manifest 307 representing the subset 203 (e.g., registry) in a concise manner". Col. 9, lines 10-43 of Ellison discusses "generating the OSNK 203 by combining the BK0 203 and the OS Nub ID 201" and "using the OSNK 203 to protect the usage of the subset 230". Thus, col. 9, lines 10-43 and col. 11, lines 40-48 of Ellison discusses subject matter unrelated to "erasing the previous secret" required in Claims 3 and 8 or "erasing the initial secret" required in Claim 15. Teal neither discusses any subject matter related to "erasing the previous secret" or "erasing the initial secret" required in Claims 3, 8 and 15. Thus, Ellison, Teal, whether alone or in a combination, does not teach or suggest "erasing the previous secret" in Claims 3 and 8 or "erasing the initial secret" in Claim 15.

The Examiner alleges that col. 9, lines 44-45 of Ellison teaches or suggests "the hash function comprises an exponentiation function" required in Claim 3, 8 and 15. However, Ellison nor Teal discusses any subject matter related to "exponentiation function" required in Claims 3, 8 and 15.

Thus, Claims 3, 8 and 15 are patentably distinct over Ellison, Teal, whether alone or in a combination. The Examiner is respectfully requested to withdraw the rejection on Claims 3, 8 and 15 under 35 U.S.C. § 103(a).

Claim 4 depends on Claim 3 and is patentable therewith. Claim 9 depends on Claim 8 and is patentable therewith.

Regarding Claims 5 and 10, the Examiner alleges that col. 7, lines 25-42 of Ellison teaches or suggests "receiving the initial secret from a system administrator" required in Claims 5 and 10. Col. 7, lines 25-42 of Ellison describes "the processor nub 18 provides the management of the symmetric key used to protect the operating system nub's secret". Figure 2 of Ellison illustrates that a key generator 240 receives BK0 202 from the processor nub 18. However, the processor nub 18 of Ellison is not a system administrator. Col. 7, lines 24-25, col. 3, lines 23 and Figure 1C of Ellison describes that the processor nub 18 is a software entity executable in a memory. Thus, Ellison fails to teach or suggest subject matter of Claims 5 and 10. Teal also fails discuss subject matter of Claims 5 and 10. Thus, Claims 5 and 10 are patentably distinct over Ellison, Teal, whether alone or in a combination.

Claims 11 and 13 depend on Claim 3 and are patentable therewith. Claim 14 depends on Claim 8 and is patentable therewith.

Regarding Claim 16, the Examiner did not state in the Office Action how Ellison or Teal teaches or suggests each limitation in Claim 16. Thus, the Examiner is respectfully requested to indicate how the Examiner finds claim limitations in Ellison and/or Teal. At least, Applicant believe that "retrieving the initial secrete via a request for entry on the initial secret by a system administrator" is not discussed in Ellison, Teal, whether alone or in a combination.

Claims 17-18 depend on Claim 15 and are patentable therewith.

Claims 24-25 are being newly added without entering new matter. Claims 24 and 25 recite "a proof of knowledge of the evolved secret equates to a cryptographic verification of a history of the administrative actions". Neither Ellison nor Teal discusses "a proof of knowledge of the evolved secret". Though Ellison discusses at col. 11, lines 26-28 "the verification process includes decrypting the retrieved signature 306 using the public key 205 to expose the before hash value", Ellison fails to discuss "a cryptographic verification of **a history of the administrative actions**". Furthermore, Ellison nor Teal does not teach or suggest "**equating** a proof of knowledge of the evolved secret **to** a cryptograph verification of a history of the administrative actions". Thus, Claims 24-25 are patentably distinct over Ellison, Teal, whether alone or in a combination.

Conclusion

In view of the foregoing, this application is now believed to be in condition for allowance, and a Notice of Allowance is respectfully requested. If the Examiner believes a telephone conference might expedite prosecution of this case, it is respectfully requested that he call the applicant's attorney at (516) 742-4343.

Respectfully submitted,

Steven Fischman
Registration No. 34,594

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

SF:JP:av